

15

WHAT IS CLAIMED IS:

1. A method for updating a first version of a program operating at a network site, comprising:

in response to an automated event, automatically downloading from a remote site any update for the program; installing a downloaded update to generate a second version of the program; and

operating the second version of the program in place of the first version at the network site.

2. The method of Claim 1, wherein the automated event is a timed event.

~~3. The method of Claim 2, further comprising:  
aging the first version of the program; and  
wherein the timed event is the first version reaching  
a specified age.~~

4. The method of Claim 3, wherein the specified age is less than or equal to ~~twenty~~ twenty-four hours.

5. The method of Claim 2, wherein the timed event occurs at least once a day.

~~6. The method of Claim 1, the act of automatically downloading from the remote site any update for the program comprising:~~

automatically connecting to the remote site in response to the automated event;

automatically determining whether the remote site includes an update for the program; and

in response to the remote site including an update,  
automatically downloading the update from the remote site.

18

4

5.13. The method of Claim 12, further comprising:

receiving a recovery event at one of the network sites;

5            automatically restoring the first version of the  
program at the network site at which the recovery event was  
received;

broadcasting a recovery message from the network site  
over the network; and

10        automatically restoring the first version of the  
     program at each of the remaining network sites operating  
     the second version of the program.

14. The method of Claim 1, wherein the program is a set of intrusion detection signatures for an intrusion detection sensor.

15. The method of Claim 1, wherein the remote site is an Internet web page.

Sub  
a5

21

Sub  
C2

22. An intrusion detection system, comprising:  
a private network including a plurality of sites  
connected to a public network, each site including an  
intrusion detection sensor operating with a first set of  
intrusion detection signatures; and

5 each of the intrusion detection sensors operable to  
automatically download from a remote site any update for  
the intrusion detection signatures in response to a  
specified event, to install a downloaded update to generate  
10 a second set of intrusion detection signatures, to operate  
with the second set of intrusion detection signatures, and  
to distribute the downloaded update to the remaining  
intrusion detection sensors for installation.

15 ~~23.~~ The system of Claim ~~22~~, wherein the specified  
event is an automated event.

~~24.~~ The system of Claim ~~23~~, wherein the automated  
event is a timed event.

20 Add a6

16

7. The method of Claim 1, further comprising downloading the update in an encrypted format and decrypting the downloaded update prior to installation.

5 8. The method of Claim 1, further comprising authenticating the downloaded update prior to installation.

*Sub 10 a 4*  
9. The method of Claim 1, further comprising:  
after installation of the downloaded update,  
determining whether the second version of the program is  
operating correctly; and

in response to incorrect operation of the second  
version, restoring the first version of the program for  
operation at the network site.

15

10. The method of Claim 1, further comprising:  
distributing the downloaded update to a disparate  
network site operating the first version of the program;  
installing the downloaded update to generate the  
second version of the program at the disparate network  
site; and

20

operating the second version of the program in place  
of the first version at the disparate network site.

062891-22874260

11. \ The method of Claim 1, further comprising:

after installation of the downloaded update,  
determining whether the second version of the program is  
operating correctly at the network site;

5           in response to incorrect operation of the second  
version, restoring the first version of the program for  
operation at the network site; and

in response to correct operation of the second version  
at the network site:

10            distributing the downloaded update to a disparate  
network site operating the first version of the program;

installing the downloaded update to generate the second version of the program at the disparate network site; and

15                   operating the second version of the program in  
place of the first version at the disparate network site.

12. The method of Claim 1, further comprising:

```

broadcasting over a network an update message;

```

20 receiving in response to the update message a request  
for the downloaded update from each of a plurality of  
disparate network sites operating the first version of the  
program;

25 distributing the downloaded update to the disparate  
network sites requesting the downloaded update;

installing the downloaded update to generate the second version of the program at each of the disparate network sites; and

operating the second version of the program in place  
30 of the first version at each of the disparate network  
sites.

19

16. A method for automatically updating an intrusion detection system having a plurality of distributed intrusion detection sensors each operating with a first set of intrusion detection signatures, comprising:

5        in response to a specified event, automatically downloading from a remote site any update for the intrusion detection signatures;

         distributing a downloaded update to each sensor;

10        installing the downloaded update to generate a second set of intrusion detection signatures for each sensor; and

         operating each sensor with the second set of intrusion detection signatures.

15        17. The method of Claim 16, wherein the specified event is a timed event.

         18. The method of Claim 17, further comprising:

         aging the first set of intrusion detection signatures;  
and

20        wherein the timed event is the first set of intrusion detection signatures reaching a specified age.

         19. The method of Claim 18, wherein the specified age is less than or equal to twenty-four hours.

25

         20. The method of Claim 17, wherein the timed event occurs at least once a day.

06280240

20

21. The method of Claim 16, the act of automatically downloading from the remote site any update for the program comprising:

5        automatically connecting to the remote site in  
     response to the timed event;

automatically determining whether the remote site includes an update for the intrusion detection signatures; and

in response to the remote site including an update,  
10 automatically downloading the update from the remote site.